PURPOSE

To establish security related requirements for hiring, transfers, terminations and related personnel actions that protect Michigan Department of Health and Human Services (MDHHS) information and information systems.

REVISION HISTORY

Issued: 10/01/2020.
Next Review: 10/01/2021.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the SOM. Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency's business.

Criminal Justice Information (CJI)

Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Electronic Protected Health Information (ePHI)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual..

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS must implement precautions to determine and ensure the suitability of employees and contractors who require access to confidential and sensitive records and information.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the personnel security [PS] family of NIST controls, managed by MDHHS in accordance with DTMB 1340.00.140.01, Personnel Security Standard. MDHHS must review this policy annually.

This policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Social Security Administration (SSA) Technical System Security Requirements (TSSR)
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

Position Risk Designation [PS-2]

MDHHS must, consistent with Michigan Civil Service Commission rules and regulations:

- Assign a risk designation to all positions.
- Establish screening criteria for individuals filling those positions.
- Review and revise risk-specific position designations annually.

Personnel Screening [PS-3]

MDHHS must, consistent with Michigan Civil Service Commission rules and regulations:

- Screen individuals prior to authorizing access to information systems.
- Rescreen individuals periodically, consistent with the criticality/sensitivity rating of the position.
- When an employee moves from one position to another, the higher level of clearance should be adjudicated.

Personnel Termination [PS-4]

Upon separation of individual employment, MDHHS must:

- Disable information system access within 24 hours, or in circumstances involving termination for cause, prior to or during the termination process.
- Terminate/revoke any authenticators/credentials associated with the individual.
- Conduct exit interviews that include a discussion of non-disclosure of information security and privacy information.
- Retrieve all security-related organizational information system-related property, including but not limited to hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes.
- Retain access to organizational information and information systems formerly controlled by the individual.
- Notify personnel determined by the immediate supervisor, information system owner, and/or MDHHS security officer, of the termination and related action(s) within 24 hours.
- Immediately escort employees terminated for cause out of the organization.

Personnel Transfer [PS-5]

MDHHS must:

- Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization.
- Initiate transfer or reassignment actions within five days following the formal action, as required for personnel transfers or reassignments to other positions, including replacement/modification of keys, identification cards and building passes, closing information accounts and establishing new accounts, modification of system access privileges, and access to official records.
- Notify personnel determined by the immediate supervisor, information system owner, and/or MDHHS security officer, of the transfer and related action(s) within 24 hours.

Access Agreements [PS-6]

MDHHS must:

- Develop and document access agreements for organizational information systems before authorizing access, including but not limited to, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.
- Review and update access agreements at least annually.
- Ensure that individuals sign appropriate access agreements, prior to being granted access, with an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized; and re-sign such agreements to maintain access when updated, or at least annually.

Third-Party Personnel Security [PS-7]

MDHHS must:

- Establish personnel security requirements including security roles and responsibilities for third-party providers.
- Require third-party providers to comply with personnel security policies and procedures established by the organization.
- Document personnel security requirements.

The account manager for each third-party provider shall notify the MDHHS security officer or other designated personnel of any transfers or terminations of third-party personnel who possess organizational credentials or badges, or who have information system privileges, as soon as transfers or terminations are known and a justification for the replacement request is submitted.

Personnel Sanctions [PS-8]

MDHHS must:

- Employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

- Notify the personnel determined by the information system owner determined by the immediate supervisor, information system owner, and/or MDHHS security officer, of the transfer and related action(s) within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Roles and Responsibilities

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding, and complying with this policy as well as supporting standards and procedures.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations:

NIST 800-53 rev.4:

PS-1 Personnel Security Policy and Procedures
PS-2 Position Risk Designation
PS-3 Personnel Screening
PS-4 Personnel Termination
PS-5 Personnel Transfer
PS-6 Access Agreements
PS-7 Third-Party Personnel Security
PS-8 Personnel Sanctions

45 CFR §164.308

164.308(a)(1)(ii)(C) Sanction Policy (R)
164.308(a)(3)(ii)(A) Authorization and/or Supervision (A)
164.308(a)(3)(ii)(B) Workforce Clearance Procedure (A)
164.308(a)(3)(ii)(C) Termination Procedure (A)
164.308(a)(4)(ii)(B) Access Authorization (A)

45 CFR §164.310

164.310(b) Workstation Use (R)
164.310(d)(2)(iii) Media Accountability (A)

45 CFR §164.314

164.314(a)(2) Business Associate Contracts (R)

State Standards/Regulations

MDHHS Policy Manuals

68E-020 Data Privacy and Security Sanctions Policy
68E-050 Termination Policy and Procedure
68E-060 Workforce Clearance Policy and Procedure
68E-070 Access Authorization Policy and Procedure

DTMB Administrative Guide

DTMB/Work Resources/Policies, Standards and Procedures/IT Technical Policies, Standards and Procedures

1340.00.140.01 Personnel Security Standard

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.